Framework for Regional Cyber Security Collaboration

Dr. Nathaniel Evans
Argonne National Laboratory

Dr. William Horsthemke
Argonne National Laboratory

Nathan Rinsema
Argonne National Laboratory

Agenda

- Introduction and Goals
- The current world
- The Regional Risk
- Collaborations and Information Sharing
- Conclusion

Goals

- Think about security in a way that gets everyone worrying and sharing information with people they trust.

Current State - Reporting a Crime

- Local Authorities
- Federal Authorities (CIC, ***, US Cert)

Common Attacks

- 0 day exploit (RDP flaw)
  - I found a hole in a system, so I am going to use it on your system
- Worked Else ware
  - This attack worked at ABC, so it might also work here as they probably don’t know it worked at ABC.
- Virus/Worm/Botnet
  - This code takes control your system and then finds others
- DDOS (Anonymous)
  - A bunch of us attack you, overwhelming you
- Social Engineering (Mitnik)
  - I pretend to be someone you trust in order to gain access

Now lets consider a focused attack

- *Draw map of city, show utilities, companies and connections.

What if we all worked together!?

- Don’t I generally trust my neighbor more then a competitor?
- Don’t I generally trust my neighbor more then the government?
- Don’t I generally trust my neighbor more then a stranger?

How would this work?

Lets see how it applies to the Common Attacks

- 0 day exploit
  - I found a hole in a system, so I am going to use it on your system
    - Your in, but hopefully not in anywhere else
- Worked Else ware
  - This attack worked at ABC, so it might also work here as they probably don’t know it worked at ABC.
    - Well ABC told me about it, so it won’t work here
- Virus/Worm/Botnet
  - This code takes control your system and then finds others
    - Well I know about that signature, so I have scanned and fixed it
- DDOS
  - A bunch of us attack you, overwhelming you
    - Yep you have overwhelmed me. However I have a separate way out through company DEF.
- Social Engineering
  - I pretend to be someone you trust in order to gain access
    - I know the FedEx guy, and you are not him.

Information sharing possibilities

Communication

- Wiki's
- Email Lists
- Chat Servers
- Meetings

Tools

- Continuous Monitoring Tools
- Cyber Federated Model

Questions? Comments? Complaints?

Sources